Quadratic Forms and the Graph Isomorphism Problem*

Shmuel Friedland
Department of Mathematics, Statistics and Computer Science
University of Illinois at Chicago
Chicago, Illinois 60680

Submitted by Richard A. Brualdi

ABSTRACT

We relate the graph isomorphism problem to the classical problem of equivalence of integer quadratic forms. We give some necessary number theoretic conditions that the isomorphic graphs have to satisfy.

1. INTRODUCTION

Let G be a graph on n vertices. Then G is represented by $0-1$ symmetric matrix $A(G)$ with zero diagonal. Two graphs G and H on n vertices are called isomorphic if $A(H)=P^TA(G)P$ for some permutation matrix P. One of the unresolved problem of complexity theory is to classify the complexity of determining if two given graphs are isomorphic. Consult [8] for a good introduction on the theory of NP-completeness, and [9] for a survey on the graph isomorphism problem. In this paper we relate the graph isomorphism problem to the classical problem of equivalence of real quadratic forms over the integers. Although we do not have any new, definite results on the graph isomorphism problem, we think that this direction of research is interesting and promising. As an example of the fruitful relation between number theory and graph theory we refer the reader to [14] and its references.

We now briefly survey the contents of this paper. Section 2 is devoted to quadratic forms over special fields—finite fields, p-adic fields, and the field

*Dedicated to Olga Taussky for unveiling to me the "mysterious" connection between number theory and matrix theory.

655 Avenue of the Americas, New York, NY 10010 0024-3795/91/$3.50

of rational numbers. In Section 3 we study quadratic forms over the integers. Most of the results of these two sections are well known. We put together the known facts on this subject in a convenient form with the references for the interested reader. Section 4—the heart of our paper—relates the graph isomorphism problem to the equivalence of quadratic forms. More precisely, Theorem 4.1 shows that the graph isomorphism problem is a special case of the equivalence of special positive definite integer quadratic forms. Section 5 is devoted to remarks, conjectures, and problems on integer quadratic forms, the graph isomorphism problem, and orthogonal similarity over the rationals.

2. QUADRATIC FORMS OVER $\mathbf{F}_q, \mathbf{Q}_p, \mathbf{Q}$

Let Γ be an integral domain. Denote by $M_n(\Gamma)$, $S_n(\Gamma)$ and $U_n(\Gamma)$ the ring of $n \times n$ matrices with entries in Γ, the set of $n \times n$ symmetric matrices with entries in Γ, and the group of $n \times n$ invertible matrices T such that $T, T^{-1} \in M_n(\Gamma)$. Let $A, B \in S_n(\Gamma)$. We say that A and B are equivalent over Γ if $B = T^T A T$ for some $T \in U_n(\Gamma)$, and denote it by $A \overset{\Gamma}{\sim} B$. Let $H \subset U_n(\Gamma)$ be a subgroup fixed under transposition: $H^T = H$. We then let $A \overset{H}{\sim} B$ if $B = T^T A T$, $T \in H$. With each $A \in S_n(\Gamma)$ we associate the quadratic form $A(x, x) = x^T A x$, $x \in \Gamma^n$, and more generally the inner product $A(x, y) = y^T A x$, $x, y \in \Gamma^n$. Then $A \overset{\Gamma}{\sim} B$ iff the corresponding quadratic forms $A(x, x)$ and $B(x, x)$ are equivalent. A $[A(x, x)]$ is called nondegenerate if $\det(A) \neq 0$. Otherwise A $[A(x, x)]$ is called degenerate. As usual let $\mathrm{orb}_\Gamma(A)$ be the class of all $B \overset{\Gamma}{\sim} A$. The basic problem in this area is to find out if $A \overset{\Gamma}{\sim} B$. This can be achieved sometime by finding a "canonical" representation $\alpha \in \mathrm{orb}_\Gamma(A)$. If $\alpha = \alpha(A)$ is unique and can be determined effectively, then $A \overset{\Gamma}{\sim} B$ iff $\alpha(A) = \alpha(B)$. This is true in many cases. However, in the more difficult cases the unique form does not exist. We now will discuss briefly certain relevant cases. We present short proofs of some known and fairly easy results. The deeper results are only stated, and references are given for the interested reader.

We first discuss the case where Γ is a field $\mathbf{F}$. Let $p = \mathrm{char}(\mathbf{F})$ be the characteristic of $\mathbf{F}$. Denote by $\mathbf{F}^*$ the multiplicative Abelian group $\mathbf{F} \setminus \{0\}$. As usual, let $\mathbf{F}^{*2}$ denote the subgroup of squares, $\{x,\ x = y^2,\ y \in \mathbf{F}^*\}$. Let $\mathbf{F}^*/\mathbf{F}^{*2}$ be the group of the quadratic residues. The following two lemmas are obvious:

LEMMA 2.1. *Let $A, B \in S_n(\mathbf{F})$ be two nondegenerate symmetric matrices. Assume that $A \overset{\mathbf{F}}{\sim} B$. Then* $\det(A)/\det(B) \in \mathbf{F}^{*2}$.

LEMMA 2.2. *Let* $A \in S_n(\mathbf{F})$ *be a degenerate quadratic form of rank* m. *Then any splitting* $\mathbf{F}^n = U \oplus \ker(A)$ *induces the splitting* $A(x,x) = A_1(y,y) \oplus 0$, $y \in U$, *where* $A_1(y,y)$ *is the unique nondegenerate quadratic form on* $\mathbf{F}^n/\ker(A)$ *induced by* $A(x,x)$. *In particular,* $A \overset{\Gamma}{\sim} B$ *iff* $\dim(\ker(B)) = n - m$ *and* $A_1 \overset{\Gamma}{\sim} B_1$.

LEMMA 2.3. *Assume that* $\operatorname{char}(\mathbf{F}) \neq 2$. *Then any* $A \in S_n(\mathbf{F})$ *is* $\mathbf{F}$*-equivalent to a diagonal matrix.*

Proof. Consider the quadratic form

$$A(x,x) = \sum_1^n a_{ij} x_i x_j.$$

Suppose first that some $a_{ii} \neq 0$. By renaming the coordinates we may assume that $a_{11} \neq 0$. Then

$$A(x,x) = a_{11}^{-1}\left(\sum_1^n a_{1i} x_i\right)^2 + A_1(y,y),\ y = (x_2, \ldots, x_n)^T. \tag{2.4}$$

If all $a_{ii} = 0$ but $a_{ij} \neq 0$ for some $i < j$, we replace the variables $x_i x_j$ by $y_i = x_i + x_j$, $y_j = x_i - x_j$ and we are in the previous case. [Note that this transformation in two variables is applicable iff $\operatorname{char}(\mathbf{F}) \neq 2$.] Finally, if $A = 0$ there is nothing to prove. Use this procedure to obtain an equivalent diagonal form to A relatively fast. ∎

We now recall the well-known results. Let $\mathbf{R}$ be the field of real numbers.

THEOREM 2.5. (Sylvester's law of inertia). *Let* $A \in S_n(\mathbf{R})$. *Then* $A \overset{\mathbf{R}}{\sim} D$ *where* D *is a diagonal matrix with entries* $\{1, -1, 0\}$. *The numbers of* $1, -1, 0$ *are uniquely determined by* A. *In particular* $S_n(\mathbf{R})$ *splits to a disjoint union of* $(n+1)(n+2)/2$ *equivalence classes.*

For $A \in S_n(\mathbf{R})$ denote by (π, ν, ζ) the inertia triple of A. That is, π, ν, ζ are the numbers of $1, -1, 0$ respectively in the above diagonal matrix $D \overset{\mathbf{R}}{\sim} A$. As usual, denote by $\sigma = \pi - \nu$ the signature of A. Let p be a prime, $q = p^m$, and denote by $\mathbf{F}_q$ the finite field with q elements. It is known that $\mathbf{F}_q^*$ is a cyclic group. Furthermore, if $p = 2$ then $\mathbf{F}_q^{*2} = \mathbf{F}_q^*$, and if $p > 2$ then and

$\mathbf{F}_q^{*2}$ is a subgroup of index two. See for example [15]. In the last case choose $\rho_q \in \mathbf{F}_q^* \setminus \mathbf{F}_q^{*2}$. As usual, let I_m be the $m \times m$ identity matrix.

THEOREM 2.6. *Let $A \in S_n(\mathbf{F}_q)$. Assume first that* $\operatorname{char}(\mathbf{F}_q) > 2$. *Then* $0 \neq A \overset{\mathbf{F}_q}{\sim} D$, *where D is a unique diagonal matrix (up to a permutation of its diagonal entries) whose first $n-1$ entries are either 0 or 1. The last entry is either 1 or ρ_q. In particular $S_n(\mathbf{F}_q)$ splits to a disjoint union of $2n+1$ equivalence classes.*

Assume that $\operatorname{char}(\mathbf{F}_q) = 2$. *Then either* $A \overset{\mathbf{F}_q}{\sim} I_m \oplus 0$ *or*

$$A \overset{\mathbf{F}_q}{\sim} \underbrace{H_2 \oplus \cdots \oplus H_2}_{m \text{ times}} \oplus 0, \qquad H_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In that case $S_n(\mathbf{F}_q)$ splits to a disjoint union $n+1+[n/2]$ equivalence classes.

Proof. For $n = 1$ the theorem is obvious. Assume that $n > 1$. According to Lemma 2.2, it is enough to consider the nondegenerate A. Suppose first that $\operatorname{char}(\mathbf{F}_q) > 2$. According to Lemma 2.3 we may assume that A is a diagonal matrix. It is left to show that any 2×2 nondegenerate diagonal matrix $\operatorname{diag}\{a, b\}$ is equivalent to a diagonal matrix $\operatorname{diag}\{1, c\}$. We claim that the equation $ax^2 + by^2 = 1$ has a solution in $\mathbf{F}_q$. Indeed, each of the two sets

$$U = \{z,\ z = ax^2,\ x \in \mathbf{F}_q\}, \qquad V = \{z,\ z = 1 - by^2,\ y \in \mathbf{F}_q\}$$

has $(q+1)/2$ distinct elements. Hence, $U \cap V \neq \varnothing$ and the above equation is solvable. Then

$$\operatorname{diag}\{1, c\} = T^T \operatorname{diag}\{a, b\}\, T, \qquad T = \begin{pmatrix} x & -by \\ y & ax \end{pmatrix},$$

and the theorem follows in this case.

Assume that $\operatorname{char}(\mathbf{F}_q) = 2$. Suppose first that all diagonal entries are equal to zero. It then follows that $A(x, x) = 0$ for all vectors $x \in \mathbf{F}_q^n$. We now choose the following orthogonal basis in $\mathbf{F}_q^n$ with respect to the inner product $A(x, y)$. Choose any $e_1 \neq 0$. Since A is nondegenerate, we must have $e_2 \neq 0$, so that $A(e_1, e_2) \neq 0$. As $A(e_1, e_1) = 0$, we deduce that e_1, e_2 are linearly independent. W.l.o.g. assume that $A(e_1, e_2) = 1$. Let $U \subset \mathbf{F}_q^n$ consist of all vectors x such that $A(x, e_1) = A(x, e_2) = 0$. Clearly, $\dim(U) \geqslant n-2$, and U

does not contain any nonzero element of the subspace $[e_1, e_2]$ spanned by e_1, e_2. Hence, $\mathbf{F}_q^n = U \oplus [e_1, e_2]$. Apply this argument to U to deduce that $n = 2m$ and $A \overset{\mathbf{F}_q}{\sim} H_2 \oplus \cdots \oplus H_2$. Assume finally that $a_{ii} \neq 0$. We claim that $A \overset{\mathbf{F}_q}{\sim} I_n$. First note that there exists e_1 such that $A(e_1, e_1) \neq 0$. Since $\mathbf{F}_q^{*2} = \mathbf{F}_q^*$, we may assume that $A(e_1, e_1) = 1$. Let $U = \{x,\ A(x, e_1) = 0\}$ be the orthogonal complement of e_1. Clearly, $\mathbf{F}_q^n = U \oplus [e_1]$. If $A(x, x)$ is not identically zero for all $x \in U$, we are done by the induction. Suppose that $A(x, x)$ is identically zero for all $x \in U$. The induction argument still works using the previous result and the observation

$$I_3 = T^T(I_1 \oplus H_2)T, \qquad T = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}. \qquad \blacksquare$$

Let p be a prime, and denote by $\mathbf{Q}_p$ the field of p-adic numbers. As usual, let $\mathbf{Q}$ stand for the rationals. In what follows we consider the quadratic forms over $\mathbf{Q}_p$ and $\mathbf{Q}$. We state without proof the classical results on this subject. A good concise reference on this topic is [15].

Let $a, b \in \mathbf{Q}_p^*$. Then the Hilbert symbol $(a, b)_p = \pm 1$ is defined as follows:

$$(a, b)_p = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution} \\ & \quad (z, x, y) \neq (0, 0, 0) \in \mathbf{Q}_p^3, \\ -1 & \text{otherwise.} \end{cases}$$

Let $D = \operatorname{diag}\{d_1, \ldots, d_n\} \in S_n(\mathbf{Q}_p)$, $n \geqslant 2$, be a diagonal nondegenerate form. We then define the Hilbert invariant:

$$\epsilon_p(D) = \prod_{1 \leqslant i < j \leqslant n} (d_i, d_j)_p = \pm 1.$$

It is known that if $D_1 \overset{\mathbf{Q}_p}{\sim} D_2$ are two nondegenerate diagonal matrices, then $\epsilon_p(D_1) = \epsilon_p(D_2)$. According to Lemma 2.3, any nondegenerate $A \in S_n(\mathbf{Q}_p)$ is equivalent to a diagonal D. Hence, we can let $\epsilon_p(A) = \epsilon_p(D)$. For simplicity of notation let $\epsilon_p(a) = 1$, $a \in \mathbf{Q}_p^*$. Recall that the group $\mathbf{Q}_p^*/\mathbf{Q}_p^{*2}$ is a finite group with eight elements for $p = 2$ and four elements for $p > 2$.

THEOREM 2.7. *Let $A, B \in S_n(\mathbf{Q}_p)$ be two nondegenerate symmetric matrices. Then $A \overset{\mathbf{Q}_p}{\sim} B$ iff $\det(A)/\det(B) \in \mathbf{Q}_p^{*2}$, $\epsilon_p(A) = \epsilon_p(B)$. Moreover,*

$\epsilon_p(A)=1$ *iff* $A \overset{\mathbf{Q}_p}{\sim} I_{n-1}\oplus\{a\}$, $a\in\mathbf{Q}_p^*$. *Furthermore, for* $n>2$ *and* $\epsilon_p(A)=-1$ *one has* $A \overset{\mathbf{Q}_p}{\sim} I_{n-3}\oplus\operatorname{diag}\{a,b,c\}$, $a,b,c\in\mathbf{Q}_p^*$. *Finally, the number of nondegenerate equivalence classes for* $p>2$ ($p=2$) *is equal to* 4 (8) *if* $n=1$, *to* 7 (15) *if* $n=2$, *and to* 8 (16) *if* $n>2$.

THEOREM 2.8. *Let* $A,B\in S_n(\mathbf{Q})$. *Then* $A \overset{\mathbf{Q}}{\sim} B$ *iff* $A \overset{\mathbf{R}}{\sim} B$ *and* $A \overset{\mathbf{Q}_p}{\sim} B$ *for all primes* p. *In particular, if* A,B *are nondegenerate,* $A \overset{\mathbf{R}}{\sim} B$, *and* $\det(A)/\det(B)\in\mathbf{Q}^{*2}$, *then* $A \overset{\mathbf{Q}}{\sim} B$ *iff* $\epsilon_p(A)=\epsilon_p(B)$ *for all primes* p.

Given a nondegenerate $A\in S_n(\mathbf{Q})$, then Hilbert's invariants satisfy the following condition:

$$\epsilon_p(A)\neq 1 \qquad \text{for a finite number of primes.} \tag{2.9}$$

For $n=2$ there is an additional condition. See for example [15, p. 44]. Furthermore, given $d\in\mathbf{Q}^*$ and numbers $\epsilon_p=\pm 1$ such that a finite number of ϵ_p are equal to -1 and two nonnegative integers π,ν, $\pi+\nu=n>2$, there exists a nondegenerate $A\in S_n(\mathbf{Q})$ with these invariants:

$$A \overset{\mathbf{R}}{\sim} I_\pi\oplus -I_\nu, \qquad \frac{\det(A)}{a}\in\mathbf{Q}^{*2}, \qquad \epsilon_p(A)=\epsilon_p, \quad p=2,3,5,\ldots.$$

For $n=2$ we have a similar result provided that the additional necessary condition holds. Thus, for $n\geqslant 3$ we can have a seminormal form for a nondegenerate $A\in S_n(\mathbf{Q})$ which basically depends on a 3×3 diagonal matrix:

THEOREM 2.10. *Let* $A\in S_n(\mathbf{Q})$, $n\geqslant 3$, *be a nondegenerate matrix with the inertia triple* $(\pi,\nu,0)$, $\pi+\nu=n$. *Then* $A \overset{\mathbf{Q}}{\sim} N\oplus\operatorname{diag}\{a,b,c\}$, $a,b,c\in\mathbf{Q}^*$, *where*

$$N=\begin{cases} I_{n-3} & \text{if} \quad \nu\leqslant 1,\\ -I_{n-3} & \text{if} \quad \pi\leqslant 1,\\ I_{\pi-2}\oplus -I_{\nu-1} & \text{if} \quad \pi\geqslant 2, \quad \nu\geqslant 2.\end{cases}$$

Proof. For $n=3$ there is nothing to prove. Assume that $n\geqslant 4$. If $\pi\geqslant n-3$, then find $B\in S_3(\mathbf{Q})$ with the inertia $(\pi-n+3,\nu,0)$ and with the invariants $\det(A)$ and $\epsilon_p(A)$, $p=2,3,5,\ldots$. We may assume that B is a

diagonal matrix. As $\epsilon_p(\mathrm{diag}\{1, a\}) = 1$, $a \in \mathbf{Q}^*$, it follows that $A \overset{\mathbf{Q}}{\sim} I_{n-3} \oplus B$. If $\nu \geqslant n-3$, use the previous result for $-A$ to deduce that $A \overset{\mathbf{Q}}{\sim} -I_{n-3} \oplus B$. Finally, if $\pi, \nu \geqslant 2$, then the above observations imply that $A \overset{\mathbf{Q}}{\sim} I_{\pi-2} \oplus B$, where $B \in S_{n-\pi+2}(\mathbf{Q})$ is a diagonal matrix with the inertia $(2, \nu, 0)$. Then the previous argument shows that $B \overset{\mathbf{Q}}{\sim} -I_{\nu-1} \oplus D$. ∎

Given $A \in S_n(\mathbf{Q})$, it is a computationally important problem to find *fast* all primes p for which $\epsilon_p(A) = -1$.

3. QUADRATIC FORMS OVER INTEGERS

Denote by $\mathbf{Z}$ the ring of integers. Let $A, B \in S_n(\mathbf{Z})$. Then $A \overset{\mathbf{Z}}{\sim} B$ iff $B = T^T A T$ for some unimodular matrix $T \in U_n(\mathbf{Z})$. In particular, $\det(A) = \det(B)$. In what follows we assume that A (B) is nondegenerate and $\det(A) = \det(B)$ unless otherwise stated. Given n and $d \in \mathbf{Z}^*$, it is known that there are only a finite number of equivalence classes of $A \in S_n(\mathbf{Z})$, $\det(A) = d$. See for example [1, §9.1]. Let p be a prime number, and denote by $\mathbf{Z}_p$ the ring of p-adic integers. That is, every $a \in \mathbf{Q}_p^*$ is the form $p^m b$, $b, b^{-1} \in \mathbf{Z}_p$, and $a \in \mathbf{Z}_p$ iff $m \geqslant 0$. It is customary to let $\mathbf{Z}_\infty = \mathbf{R}$. Clearly

$$A \overset{\mathbf{Z}}{\sim} B \quad \Rightarrow \quad A \overset{\mathbf{Z}_p}{\sim} B, \quad p = 2, 3, 5, \ldots, \infty.$$

One says that A and B belong to the same genus and denote it by $A \overset{\mathrm{loc}}{\sim} B$ if the RHS of the above condition holds. $A \in S_n(\mathbf{Z})$ is called *type* (II) if all diagonal entries are divisible by 2. Otherwise A is called *type* (I). The following result is well known, (e.g. [1, §8.3–8.4]) and is an extension of Theorem 2.6.

THEOREM 3.1. *Let* $A, B \in S_n(\mathbf{Z})$, $\det(A) = \det(B)$. *Assume that* p *is a prime and* p *does not divide* $\det(A) = \det(B)$. *Then* $A \overset{\mathbf{Z}_p}{\sim} B$ *if either* $p > 2$ *or* $p = 2$ *and* A, B *are both of type* (II).

Let $A \in S_n(\mathbf{Z})$, and denote by $\mathrm{genus}(A)$ the set of all $B \overset{\mathrm{loc}}{\sim} A$. Then $\mathrm{genus}(A)$ can be subdivided to finer classes $\mathrm{spin}(A)$—the spinor genera—by introducing the Clifford algebra corresponding to a nondegenerate inner product $A(x, y)$. The number of spinor genera in a given genus is finite and

is a power of 2. If $p^{\delta(p,n)} \nmid \det(A)$ for every prime p, then genus(A) contains one spinor genus. See [1, Theorem 1.5, p. 203]. Here

$$\delta(2,n) = \frac{n(n-3)}{2} + \left[\frac{n+1}{2}\right], \qquad \delta(p,n) = \frac{n(n-1)}{2} \quad \text{for } p > 2. \tag{3.2}$$

The "spin" invariant of A is also considered to be "local" invariant. Recall that $A \in S_n(\mathbf{R})$ is called indefinite if the first two numbers in the inertia triple (π, ν, ζ) are different from zero. The following theorem gives the exact conditions under which local implies global. See for example [1, §11.1].

THEOREM 3.3. *Let $n \geqslant 3$, and assume that $A \in S_n(\mathbf{Z})$ is a nondegenerate indefinite matrix. Then $B \overset{\mathbf{Z}}{\sim} A \Leftrightarrow B \in \text{spin}(A)$.*

We now discuss in detail the unimodular forms, i.e. $A \in S_n(\mathbf{Z})$, $\det(A) = \pm 1$. Note that if the inertia triple of a symmetric unimodular A is $(\pi, \nu, 0)$, then $\det(A) = (-1)^\nu$. Clearly, the matrix $I_\pi \oplus -I_\nu$ is a unimodular matrix of type (I) with prescribed inertia triple $(\pi, \nu, 0)$. We now consider type (II) unimodular matrices. Clearly, the 2×2 matrix H_2 introduced in Theorem 2.6 is type (II) with zero signature. Hence, $H_2 \oplus \cdots \oplus H_2$ is a type (II) unimodular matrix of even dimension with $\sigma = 0$. It is known that the signature of type (II) unimodular matrix is divisible by 8. See for example [1]. The following matrix is a type (II) positive definite unimodular matrix.

$$\begin{aligned} E_8 &= (e_{ij})_1^8, \\ e_{ii} &= 2, \\ e_{pq} = e_{qp} &= -1, \qquad \text{either } q = p+1,\ p = 1, \ldots, 6, \text{ or } p = 5,\ q = 8, \\ e_{pq} &= 0 \qquad\quad \text{otherwise.} \end{aligned} \tag{3.4}$$

The following is known (e.g. [15]):

THEOREM 3.5. *Let $A, B \in S_n(\mathbf{Z})$ be two indefinite unimodular matrices. Then $A \overset{\mathbf{Z}}{\sim} B$ iff A and B have the same type and the same inertia. In particular, if $A \in S_n(\mathbf{Z})$ is indefinite and unimodular, then A is $\mathbf{Z}$ equivalent*

either to the type (I) matrix $I_\pi \oplus -I_\nu$, $\pi, \nu \geqslant 1$, *or to one of the type (II) matrices*

$$H_2 \oplus \cdots \oplus H_2, \qquad \underbrace{H_2 \oplus \cdots \oplus H_2}_{m \geqslant 1 \text{ times}} \oplus E_8 \oplus \cdots \oplus E_8,$$

$$\underbrace{H_2 \oplus \cdots \oplus H_2}_{m \geqslant 1 \text{ times}} \oplus -E_8 \oplus \cdots \oplus -E_8.$$

LEMMA 3.6. *Let* $A, B \in S_n(\mathbf{Z})$ *be two unimodular matrices having the same type and inertia. Then* A *and* B *belong to the same genus and hence to the same spinor genus.*

Proof. If A, B are type (II), then this lemma is a consequence of Theorem 3.1. If A, B are indefinite, then this lemma is a consequence of Theorem 3.5. It is enough to consider the case where A, B are positive definite type (I) matrices. Theorem 3.1 yields that $A \overset{\mathbf{Z}_p}{\sim} B$ for $p > 2$. According to Theorem 3.5 $A \oplus -I_1 \overset{\mathbf{Z}}{\sim} B \oplus -I_1$. In particular $A \oplus -I_1 \overset{\mathbf{Z}_2}{\sim} B \oplus -I_1$. Then the appropriate generalization of Witt's lemma [1, Chapter 8, Lemma 4.2] implies that $A \overset{\mathbf{Z}_2}{\sim} B$. ∎

It is possible to prove Lemma 3.6 directly without invoking Theorem 3.5. In that case Theorem 3.5 follows from Lemma 3.6 and Theorem 3.3 for $n \geqslant 3$.

The (positive) definite unimodular forms (matrices) $A(x, x)$ have much richer structure. According to Eichler, e.g. [13, §2.6], definite unimodular forms decompose uniquely (up to a permutation of factors) to a direct sum of indecomposable definite unimodular forms. For $n \leqslant 7$ there is one equivalence class (given by the identity matrix). For $n = 8$ one has two classes—orb(I_8), orb(E_8). Kneser showed that there are exactly seven indecomposable nonequivalent positive definite unimodular matrices for $n \leqslant 16$. The number of equivalence classes of definite unimodular matrices seems to grow exponentially with n. See [13] or [15]. Thus, the complete classification of definite unimodular matrices for general n is considered to be impossible. In what follows we give a seminormal form for a unimodular positive definite matrix with at most three eigenvalues different from 1. See [5] for details.

THEOREM 3.7. *Let* $A(x, x)$ *and* $B(x, x)$ *be two positive definite integer unimodular forms. Then* A *and* B *are equivalent over integers to* $A_1 = (a_{ij})_1^n$

and $B_1 = (b_{ij})_1^n$ *respectively, so that* $a_{ij} = b_{ij}$, $1 \leqslant i, j \leqslant n-2$. *Furthermore,* B *is equivalent to the matrix*

$$(I + \tau f g^T)(I + \tau g f^T) - hh^T, \qquad \tau \neq -1, \quad f^T g = 1,$$

$$(\tau+1)^2(1 - h^T h) + 2\tau(\tau+1)(h^T g)(h^T f) - \tau^2 (h^T g)^2 (f^T f) = 1.$$

Here, τ *is an integer, and* f, g, *and* h *are column vectors with* n *integer coordinates. It follows that the above matrix has at least* $n-3$ *eigenvalues equal to* 1.

We deduce Theorem 3.7 by carefully analyzing the equivalent indefinite forms $A \oplus -I_1$ and $B \oplus -I_1$. In this analysis the use of the Smith normal form is crucial. If A and B are positive definite unimodular matrices of the same type, then Lemma 3.6 and Theorem 3.3 yield that $A \oplus (-a) \overset{\mathbf{Z}}{\sim} B \oplus (-a)$ for any $a \geqslant 1$, $p^{\delta(p,n)} \nmid a$, $p = 2, 3, 5, \ldots$. In that case we conjecture that the matrices A_1, B_1 in Theorem 3.7 can be chosen to have the same principal submatrix of order $n-1$. Furthermore, we conjecture that if $B \notin \mathrm{orb}(I_n)$ is of type (I) then B is equivalent to a matrix with $n-2$ eigenvalues equal to 1. Consult also with the recent results of [2, Chapter 26].

Let $A \in S_n(\mathbf{Z})$ be a positive definite matrix. That is, $x^T A x > 0$ for $0 \neq x \in \mathbf{R}^n$. Then A is equivalent to a Minkowski reduced form $B \in S_n(\mathbf{Z})$, which can be found as follows. Consider the lattice $\mathbf{Z}^n$ with the inner product $(x, y) = y^T A x$. First, find the shortest nonzero vector in this lattice with respect to the above metric:

$$\min_{0 \neq x \in \mathbf{Z}^n} x^T A x = e_1^T A e_1. \tag{3.8}$$

(Note that e_1 does not have to be unique.) Clearly, $e_1 = (e_{11}, \ldots, e_{1n})^T$ is primitive. That is, $\gcd(e_{11}, \ldots, e_{1n}) = 1$, and e_1 can be completed to a basis in $\mathbf{Z}^n$. Assume that we have found k vectors $e_1, \ldots, e_k$, $1 \leqslant k < n$, which form the first k vectors in the preferred basis of $\mathbf{Z}^n$. W.l.o.g. we may assume that $e_i = (\delta_{i1}, \ldots, \delta_{in})^T$, $i = 1, \ldots, k$. Then e_{k+1} is a solution to the minimal problem

$$\min_{x = (x_1, \ldots, x_n)^T \in \mathbf{Z}^n,\ \gcd(x_{k+1}, \ldots, x_n) = 1} (x, x) = (e_{k+1}, e_{k+1}). \tag{3.9}$$

In the Minkowski reduced basis the inner product (x, y) is represented by $y^T B x$. It is known that A has a finite number of Minkowski reduced forms. In many cases the Minkowski reduced basis is unique. Hence the Minkowski

reduced form is unique. See for example [1, Chapter 12]. However, in the most interesting cases from our point of view the Minkowski form is never unique, as we shall see in the next section.

4. PERMUTATIONAL EQUIVALENCE

Denote by Π_n the group of $n \times n$ permutation matrices. Let $A, B \in S_n(\Gamma)$. We say that A, B are permutationally equivalent, and denote it by $A \approx B$, if $B = P^T A P$, $P \in \Pi_n$. It is straightforward to show that permutational equivalence over any integral domain Γ is equivalent to permutational equivalence of $A, B \in S_n(\mathbf{Z}_+)$. Here we denote by $\mathbf{Z}_+$ and $S_n(\mathbf{Z}_+)$ the sets of nonnegative integers and nonnegative symmetric matrices with integer entries respectively. Indeed, for $A \in S_n(\Gamma)$ denote by $\omega(A)$ the set of distinct elements composed of the elements of A. Suppose that $A \approx B$. Then $\omega(A) = \omega(B) = \{\alpha_1, \ldots, \alpha_k\}$. Let $C, D \in S_n(\mathbf{Z}_+)$ be the matrices obtained from A, B by replacing the entries equal to α_j with $j-1$ for $j = 1, \ldots, k$. Clearly, $A \approx B \Leftrightarrow C \approx D$. Denote by $O_n(\mathbf{Z})$ the orthogonal group of $n \times n$ matrices over the integers. That is, $T \in O_n(\mathbf{Z})$ iff $T = PD$ where $P \in \Pi_n$ and D is a diagonal matrix with the diagonal entries equal to ± 1. Let $A, B \in S_n(\mathbf{Z})$. Recall that $A \overset{O(\mathbf{Z})}{\sim} B$ iff $B = T^T A T$, $T \in O_n(\mathbf{Z})$. Note that in this case A, B are similar over $\mathbf{R}$. Hence, A, B have the same characteristic polynomial. Also, $A \overset{O(\mathbf{Z})}{\sim} B \Leftrightarrow A + \lambda I_n \overset{O(\mathbf{Z})}{\sim} B + \lambda I_n$. Clearly, $A \approx B \Rightarrow A \overset{O(\mathbf{Z})}{\sim} B$. On the other hand, if all nonzero off-diagonal entries of A and B have the same sign, then a straightforward argument shows the equivalence $A \approx B \Leftrightarrow A \overset{O(\mathbf{Z})}{\sim} B$. For $A \in S_n(\mathbf{R})$ let $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$ be the eigenvalues of A. Assume that $A \in S_n(\mathbf{Z}_+)$. Then Perron's theorem implies that $\lambda_1(A) \geqslant -\lambda_n(A)$. If A is an irreducible matrix, then $\lambda_n(A) = -\lambda_1(A)$ iff A^2 is a reducible matrix. That is, the irreducible graph induced by A is bipartite. The following theorem relates the permutational equivalence to the equivalence over the integers:

THEOREM 4.1. *Let $A, B \in S_n(\mathbf{Z})$ have the same characteristic polynomial. Assume furthermore that*

$$0 < \lambda_1(A) < 2\lambda_n(A). \tag{4.2}$$

Suppose that $A \overset{\mathbf{Z}}{\sim} B$. Then $A \overset{O(\mathbf{Z})}{\sim} B$. If in addition the nonzero off-diagonal elements of A and B have the same sign, then $A \approx B$.

Proof. The condition (4.2) yields that A and B are positive definite matrices. Suppose that $B = T^T A T$. Let $x \in \mathbf{Z}^n$ be a column of T. So $x^T A x$ is a some diagonal entry b_{ii} of B. Thus,

$$\lambda_1(B) \geqslant b_{ii} = x^T A x \geqslant \lambda_n(A) x^T x \quad \Rightarrow \quad 2 > x^T x.$$

As x is a nonzero vector with integer coordinates, it follows that all the coordinates of x except one are equal to 0. The nonzero coordinate is ± 1. Since T is an invertible matrix, we deduce that $T \in O_n(\mathbf{Z})$. Assume in addition that the nonzero off-diagonal entries of A and B have the same sign. Note that $T = PD$, $P \in \Pi_n$, and D is a diagonal matrix with ± 1 on its diagonal. It then follows that $B = P^T A P$. ∎

Recall that $A \in S_n(\mathbf{R})$ is called an M-matrix if A is nonnegative definite $[\lambda_n(A) \geqslant 0]$ and all off-diagonal entries of A are nonpositive. For example, the matrix E_8 given by (3.4) is an M-matrix. For $A \in S_n(\mathbf{Z})$ let $r_i(A)$ be the ith row sum of A. Set $R(A) = \max r_i(A)$. Let

$$L(A) = \operatorname{diag}\{r_1(A), \ldots, r_n(A)\} - A, \qquad A \in S_n(\mathbf{Z}) \tag{4.3}$$

be the Laplacian matrix corresponding to A. It is straightforward to check that $A \approx B \Leftrightarrow L(A) \approx L(B)$. The advantage in introducing $L(A)$ is that $L(A)e = 0$, where $e = (1, \ldots, 1)^T$. Assume that $A \in S_n(\mathbf{Z}_+)$. Then the following facts are well known: $|\lambda_i(A)| \leqslant R(A)$. If A is irreducible, then we have strict inequalities for all i unless $Ae = R(A)e$. The matrix $L(A)$ is a singular M-matrix. If A is irreducible, then 0 is a simple eigenvalue of $L(A)$. The following lemma is straightforward, and its proof is left to the reader:

LEMMA 4.4. *Let $C \in S_n(\mathbf{Z})$. Assume that $\lambda > \max\{-\lambda_1(A), \lambda_1(A) - 2\lambda_n(A)\}$, $\lambda \in \mathbf{Z}$. Then the matrix $C + \lambda I_n$ satisfies the condition* (4.2). *In particular, if $C \in S_n(\mathbf{Z}_+)$, then for $\lambda > 3R(A)$ $(\lambda > 2R(A))$ the matrix $C + \lambda I_n$ $(L(A) + \lambda I_n)$ satisfies the condition* (4.2). *If in addition A is irreducible and either $Ae \neq R(A)e$ or $Ae = R(A)e$ and the graph corresponding to A is not bipartite, then it is enough to choose $\lambda = 3R(A)$ $(= 2R(A))$.*

LEMMA 4.5. *Let $A \in S_n(\mathbf{Z})$ be a positive definite matrix satisfying the condition* (4.2). *Assume that $e_1, \ldots, e_n \in \mathbf{Z}^n$ is a Minkowski basis for A. Then for some choice of the signs, $\{\pm e_1, \ldots, \pm e_n\}$ is a permutation of the standard basis in $\mathbf{Z}^n$.*

Proof. Note that if $x^T x = 1$ then $x^T Ax \leqslant \lambda_1(A)$. On the other hand, if $x^T x \geqslant 2$ then $x^T Ax \geqslant \lambda_n(A) x^T x > \lambda_1(A)$. ■

Assume that A satisfies the assumptions of Lemma 4.5. If all the diagonal entries of A are pairwise distinct, then the Minkowski basis is unique (up to a sign in each basis element). On the other hand, if all the diagonal entries are equal, then the ambiguity of the Minkowski basis is precisely up to the action of Π_n.

Let G be a simple undirected graph on n vertices. Then G is represented by 0-1, $n \times n$ symmetric matrix $A = A(G)$ with zero diagonal. The representation matrix A is unique up to permutational equivalence. One yet unresolved problem in the theory of computation is whether the problem of determining when given two 0-1 symmetric matrices A, B with zero diagonal are permutationally equivalent is NP-complete. Consult [8] for a good introduction to the theory of NP-completeness and [9] for a survey on the graph isomorphism problem. Roughly speaking, it is the problem of determining if $A \approx B$ is fast (polynomial in n) or not. Note that since $A(G)$ has zero diagonal, then for any matrix $A(G) + \lambda I_n$ which satisfies the conditions of Lemma 4.5, the Minkowski basis consists of all possible permutations of the standard basis. If G is not regular $[A(G)e \neq R(A(G))e]$ or G is regular but not bipartite, we can choose $\lambda = 3R(A(G))$. Here $R(A(G))$ is the maximal degree of the vertices of G. On the other hand, we can also consider the Laplacian matrix $L(A(G))$. Here, the diagonal entries form the degree sequence of G. Then a Minkowski basis of $L(A(G)) + \lambda I_n$ is determined up to a permutation between the vertices with the same degrees. So if G is regular, the ambiguity is again up the action of Π_n.

We now point out to a few "local" tests for $A \approx B$. Clearly, the matrices A and B belong to the same similarity class over the unimodular matrices $U_n(\mathbf{Z})$. However, the problem of determining if A and B are similar over $U_n(\mathbf{Z})$ does not seem to be a simple problem either. We now describe a known result which is less then unimodular similarity but is easy to verify.

Let Γ be a Euclidean domain, and assume that $A, B \in M_n(\Gamma)$. The relatively easy problem to solve over Γ is the conjugacy problem. We say that $A, B \in M_n(\Gamma)$ are conjugate and denote it by $A \overset{\Gamma}{\simeq} B$ if $B = QAT$, $Q, T \in U_n(\Gamma)$. That is, A and B have the same Smith normal form over Γ. Clearly,

$$A \approx B \quad \Rightarrow \quad A + \lambda I_n \overset{\Gamma}{\simeq} B + \lambda I_n \quad \forall \lambda \in \Gamma. \tag{4.6}$$

We do not know what kind of conditions the RHS of (4.6) implies on (A, B). Consider the following linear operator on $M_n(\Gamma)$: $X \mapsto AX - XB$. It is well

known that this operator is represented by the matrix $I\otimes A - B^T\otimes I$. A simple computation shows that if A and B are similar over Γ, i.e. $B = T^{-1}AT$, $T \in U_n(\Gamma)$, then

$$I\otimes A - A^T\otimes I \overset{\Gamma}{\simeq} I\otimes A - B^T\otimes I \overset{\Gamma}{\simeq} I\otimes B - B^T\otimes I. \tag{4.7}$$

Furthermore, (4.7) implies that A and B are similar over the quotient field $\mathbf{F}$ of Γ. See [4, Theorem 3.3]. In particular, if $A, B \in S_n(\mathbf{Z})$ are permutationally equivalent, then

$$I\otimes A - A\otimes I \overset{\mathbf{Z}}{\simeq} I\otimes A - B\otimes I \overset{\mathbf{Z}}{\simeq} I\otimes B - B\otimes I. \tag{4.8}$$

The above condition is fast to check. Of course, if $A \approx B$, then the above three matrices are also permutationally equivalent. But this is the problem we are trying to simplify! Note that (4.8) yield that

$$I\otimes A - A\otimes I \overset{\mathbf{F}_p}{\simeq} I\otimes A - B\otimes I \overset{\mathbf{F}_p}{\simeq} I\otimes B - B\otimes I. \tag{4.9}$$

Here, $\mathbf{F}_p$ is the residue field modulo prime p. Hence, A and B are similar over $\mathbf{F}_p$. That is, $\exists T \in M_n(\mathbf{Z})$, $AT - TB = 0$, $\mathrm{p} \nmid \det(T)$. It then follows that $T \in U_n(\mathbf{Z}_p)$. Hence, we deduce:

THEOREM 4.10. *Let $A, B \in S_n(\mathbf{Z})$ satisfy the condition* (4.8). *Then A, B are similar over $\mathbf{Z}_p$, $p = 2, 3, \ldots, \infty$.*

In what follows we assume that $A, B \in S_n(\mathbf{Z})$ satisfy (4.8). We now apply some of the results of previous sections to the problem of permutational equivalence of A, B. Clearly,

$$A \approx B \quad \Rightarrow \quad A + \lambda I_n \overset{\mathbf{Z}}{\sim} B + \lambda I_n \quad \forall \lambda \in \mathbf{Z} \quad \Rightarrow \quad A + \lambda I_n \overset{\mathbf{Z}_p}{\sim} B + \lambda I_n \quad \forall \lambda \in \mathbf{Z}. \tag{4.11}$$

Assume first that $p > 2$. Then, according to Theorem 3.1, if $p \nmid \det(A + \lambda I_n)$, then the third condition of (4.11) is satisfied. Note that if all the diagonal entries of A, B and λ have the same parity, then we can still use Theorem

3.1 for $p = 2$. We say that a prime p is critical if A and B have eigenvalues in $\mathbf{F}_p$ considered as matrices in $S_n(\mathbf{F}_p)$. That is,

$$\exists \lambda \in \mathbf{Z}, \qquad p \mid \det(A + \lambda I_n). \tag{4.12}$$

It then follows that we should check the last condition of (4.11) only for p, λ satisfying (4.12). Note that if A does not have integer eigenvalues, then the number of critical primes is finite. [It will be the subset of all primes for which at least one irreducible factor of $\det(A + \lambda I_n)$ over $\mathbf{Z}$ splits over $\mathbf{F}_p$.] On the other hand, if λ is an integer eigenvalue of A, then every prime p is critical. Hence, in permutational equivalence we should consider the splitting of $\det(A + \lambda I_n)$ over the integers and the corresponding splitting of $\mathbf{Z}^n$ into the direct sum of the invariant eigenspaces. We elaborate this aspect very briefly. Consult [7, Chapter 7] for further discussion.

Let $A \in S_n(\mathbf{Z})$. Set

$$\det(\lambda I_n - A) = \phi_1(\lambda)^{m_1} \cdots \phi_k(\lambda)^{m_k}, \qquad \phi_i(\lambda) \in \mathbf{Z}[\lambda],\ (\phi_i, \phi_j) = 1,$$

$$i \neq j = 1, \ldots, k, \tag{4.13}$$

$$X_i = \{x,\ x \in \mathbf{Z}^n,\ \phi_i(A)x = 0\}, \qquad i = 1, \ldots, k.$$

That is, X_i is the invariant sublattice of A corresponding to the irreducible factor $\phi_i(\lambda)$ of the characteristic polynomial of A. The trivial example of 2×2 matrix with all entries equal 1 shows that in general $X_1 \oplus \cdots \oplus X_k \neq \mathbf{Z}^n$. Let $e_{i1}, \ldots, e_{in_i} \in \mathbf{X}_i$ be a basis of the lattice X_i. Then $e_{11}, \ldots, e_{kn_k}$ forms a basis in $\mathbf{Q}^n$. Furthermore, $e_{is}^T e_{jt} = 0$ for $i \neq j$. Assume that $B \in S_n(\mathbf{Z})$ has the same characteristic polynomial as A. Let $Y_1, \ldots, Y_k \subset \mathbf{Z}^n$ be the invariant sublattices of B corresponding to irreducible polynomials $\phi_1(\lambda), \ldots, \phi_k(\lambda)$ respectively. Let $f_{i1}, \ldots, f_{in_i}$ be a basis of Y_i for $i = 1, \ldots, k$. Set

$$E_i = \left(e_{is}^T e_{it}\right)_{s,t=1}^{n_i}, \qquad F_i = \left(f_{is}^T f_{it}\right)_{s,t=1}^{n_i},$$

$$Ae_{is} = \sum_{t=1}^{n_i} a_{st}^{(i)} e_{it}, \qquad A_i = \left(a_{st}^{(i)}\right)_{s,t=1}^{n_i},$$

$$Bf_{is} = \sum_{t=1}^{n_i} b_{st}^{(i)} f_{it}, \qquad B_i = \left(b_{st}^{(i)}\right)_{s,t=1}^{n_i}. \tag{4.14}$$

Note that the matrices A_iE_i, B_iF_i are symmetric. It is straightforward to deduce:

THEOREM 4.15. *Let $A, B \in S_n(\mathbf{Z})$. Assume that $A \approx B$. Let E_i, F_i, A_i, B_i, $i = 1, \ldots, k$, be defined as above. Then*

$$\mu A_iE_i + \lambda E_i \overset{\mathbf{Z}}{\sim} \mu B_iF_i + \lambda F_i, \qquad \forall \mu, \lambda \in \mathbf{Z}, \quad i = 1, \ldots, k. \tag{4.16}$$

In particular

$$\det(A_iE_i + \lambda E_i) = \det(B_iF_i + \lambda F_i), \qquad i = 1, \ldots, k. \tag{4.17}$$

We remark that under the assumption of Theorem 4.15 the three symmetric matrices appearing in (4.8) are permutationally equivalent. Hence we can apply Theorem 4.15 to these three matrices. Note that the matrix $I \otimes A - A \otimes I$ has a trivial eigenvalue. The sublattice corresponding to $\phi_1(\lambda) = \lambda$ is the lattice of all integer valued matrices commuting with A.

5. REMARKS AND OPEN PROBLEMS

Let $A \in S_n(\mathbf{Z})$ be a positive definite matrix. We then can associate with A the theta function

$$\Theta(t, A) = \sum_{x \in \mathbf{Z}^n} e^{\pi i t x^T A x}.$$

The above series converge for $\operatorname{Im} t > 0$.It is trivial to see that if $A \overset{\mathbf{Z}}{\sim} B$ then $\Theta(t, A) = \Theta(t, B)$. If we let $q = e^{\pi i t}$, then for $\operatorname{Im} t > 0$ the above theta function has a power series in q such that the coefficient of q^m is the number of distinct representations $m = x^T A x$, $x \in \mathbf{Z}^n$. Recently, some deep results in graph theory were obtained using the theta function. See [14] and the references there.

For the permutational equivalence it is obvious that one has to consider a theta function in two variables:

$$\Theta(s, t, A) = \sum_{x \in \mathbf{Z}^n} e^{\pi i (t x^T A x + s x^T x)}, \qquad \operatorname{Im} t > 0, \quad \operatorname{Im} s \geqslant 0.$$

Again, if $A \overset{O(\mathbf{Z})}{\sim} B$ then $\Theta(s, t, A) = \Theta(s, t, B)$. We now expand this approach slightly without using the theta functions explicitly.

Let

$$S^{n,m} = \{x,\ x \in \mathbf{Z}^n,\ x^T x = m \in \mathbf{Z}_+\}.$$

Let $A \in S_n(\mathbf{Z})$. Then $A : S^{n,m} \to \mathbf{Z}$ is given by $x \mapsto x^T A x$. Assume that $A, B \in S_n(\mathbf{Z})$. We let $A \overset{m}{\asymp} B$ if the two discrete maps $A : S^{n,m} \to \mathbf{Z}$, $B : S^{n,m} \to \mathbf{Z}$ are conjugate. That is, for any $t \in \mathbf{Z}$ the sets

$$\{x,\ x \in \mathbf{Z}^n,\ x^T x = m,\ x^T A x = t,\}, \qquad \{x,\ x \in \mathbf{Z}^n,\ x^T x = m,\ x^T B x = t\}$$

have the same cardinality. We let $A \asymp B$ if $A \overset{m}{\asymp} B$ $\forall m \in \mathbf{Z}_+$. Clearly, $A \overset{\mathrm{O}(\mathbf{Z})}{\sim} B \Rightarrow A \asymp B$. We conjecture

CONJECTURE 5.1. Let $A, B \in S_n(\mathbf{Z})$. Then $A \asymp B \Rightarrow A \overset{\mathrm{O}(\mathbf{Z})}{\sim} B$.

Numerically, to find whether $A \asymp B$ one checks the conditions

$$A \overset{m}{\asymp} B, \qquad m = 1, \ldots, k. \tag{5.2}$$

Assume that $A = A(G)$, $B = B(H)$, where G and H are graphs. Suppose furthermore that $R(A(G)) = R(B(G)) \leqslant d$ where d is fixed. It may be possible that there exists $\delta = \delta(d)$ such that if the condition (5.2) holds for $k = \delta(d)$ we deduce that $A \asymp B$. If also Conjecture 5.1 held, we would obtain an alternative proof to the result of [12].

The condition (5.2) extends conveniently to simultaneous equivalence. Let $A_1, \ldots, A_l, B_1, \ldots, B_l \in S_n(\mathbf{Z})$. Denote

$$(A_1, \ldots, A_l) \overset{\mathrm{O}(\mathbf{Z})}{\sim} (B_1, \ldots, B_l) \quad \Leftrightarrow \quad B_i = T^T A_i T, \quad i = 1, \ldots, l,\ T \in \mathrm{O}_n(\mathbf{Z}),$$

$$(A_1, \ldots, A_l) \approx (B_1, \ldots, B_l) \quad \Leftrightarrow \quad B_i = T^T A_i T, \quad i = 1, \ldots, l,\ T \in \Pi_n.$$

An l-tuple $(A_1, \ldots, A_l)$ defines a discrete map

$$(A_1, \ldots, A_l) : S^{n,m} \to \mathbf{Z}^l, \qquad x \mapsto \left(x^T A_1 x, \ldots, x^T A_l x\right).$$

We then let $(A_1, \ldots, A_l) \overset{m}{\asymp} (B_1, \ldots, B_l)$ if for any $(t_1, \ldots, t_l) \in \mathbf{Z}^l$ the following

two sets have the same cardinality:

$$\{x,\ x \in \mathbf{Z}^n,\ x^T x = m,\ x^T A_i x = t_i,\ i = 1,\dots,l\},$$

$$\{x,\ x \in \mathbf{Z}^n,\ x^T x = m,\ x^T B_i x = t_i,\ i = 1,\dots,l\}.$$

Let

$$(A_1,\dots,A_l) \asymp (B_1,\dots,B_l) \quad \Leftrightarrow \quad (A_1,\dots,A_l) \overset{m}{\asymp} (B_1,\dots,B_l) \quad \forall m \in \mathbf{Z}_+.$$

Finally, from a computational point of view we have a similar condition to (5.2):

$$(A_1,\dots,A_l) \overset{m}{\asymp} (B_1,\dots,B_l), \qquad m = 1,\dots,k. \tag{5.3}$$

According to our recent results [6], simultaneous permutational equivalence is closely related to permutational equivalence. Indeed, let $A, B \in S_n(\mathbf{Z})$. In [6] we show that $A \approx B \Leftrightarrow (A_1,\dots,A_l) \approx (B_1,\dots,B_l)$, where $A_1,\dots,A_l$ and $B_1,\dots,B_l$ represent two sets of edge disjoint graphs which partition the complete graph on n vertices in a very special way. Using Theorem 4.1 and its proof, we state a natural extension of Conjecture 5.1:

CONJECTURE 5.4. Let $A_1,\dots,A_l, B_1,\dots,B_l \in S_n(\mathbf{Z})$ be 0-1 matrices. Then

$$(A_1,\dots,A_l) \asymp (B_1,\dots,B_l) \quad \Rightarrow \quad (A_1,\dots,A_l) \approx (B_1,\dots,B_l).$$

So far we have showed how the graph isomorphism problem can be treated in terms of equivalence of quadratic forms over the integers. We now show how the results on the graph isomorphism problem give rise to interesting results on the integer quadratic forms. Consider an n dimensional lattice L_n. We can identify this lattice with $\mathbf{Z}^n$. Then a metric on L_n is induced by the inner product $(x, y) = y^T A x$, $x, y \in \mathbf{Z}^n$. Here, $A \in S_n(\mathbf{Z})$ is a positive definite matrix. The unresolved complexity problem is finding the shortest nonzero vector in L_n, that is, $\min_{0 \neq x \in \mathbf{Z}^n} x^T A x$. See for example [10]. This problem is exactly the problem of finding the first vector in Minkowski's reduced basis that we discussed briefly in Section 3. Recall that an NP-hard problem is a computational problem which is at least as complex as an NP-complete problem.

THEOREM 5.5. *The problem of finding the Minkowski basis for a positive definite integer valued matrix is NP-hard.*

Proof. Let $A = A(G)$, and consider the problem of finding a permutation matrix P with zero diagonal so that $P^TAP = A$ That is, we are asking if the group of automorphisms of the graph G contains an automorphism which does not fix any vertex of G. It is known that this problem is NP-complete [11]. It is left to show that by finding the Minkowski basis of a certain positive matrix $B \in S_N(\mathbf{Z})$ we can find out if G has an automorphism with no fixed points. Considering the following sublattice $L_N \subset M_n(\mathbf{Z}) \times \mathbf{Z}$:

$$L_N = \{(X,t),\ X = (x_{ij})_1^n \in M_n(\mathbf{Z}),\ x_{ii} = 0,\ i = 1,\ldots,n,\ t \in \mathbf{Z},$$

$$Xe = X^Te = te,\ AX - XA = 0\}. \quad (5.6)$$

Here, $e = (1,\ldots,1)^T$. For $(X,t),(Y,s) \in L_N$ we let $((X,t),(Y,s)) = \operatorname{trace}(XY^T)$. It then follows that this inner product is positive. Let $(X_1,t_1),\ldots,(X_N,t_N)$ be the Minkowski basis of this inner product. Suppose that (X_i,t_i) is the first vector in the Minkowski basis such that $t_i \neq 0$. Then it is straightforward to check that G has an automorphism with no fixed points iff $\operatorname{trace}(X_iX_i^T) = n$. In particular, $t_i = \pm 1$. ∎

We close this paper with a problem which is slightly more restrictive than a rational equivalence. Let $A, B \in S_n(\mathbf{Q})$. We let $A \overset{O(\mathbf{Q})}{\sim} B$ if $B = T^TAT$, $T \in O_n(\mathbf{Q})$. That is, T is a orthogonal matrix with rational entries. Clearly, if $A \overset{O(\mathbf{Q})}{\sim} B$, then A and B have the same characteristic polynomial.

PROBLEM 5.7. Let $A, B \in S_n(\mathbf{Q})$ have the same characteristic polynomial. When is $A \overset{O(\mathbf{Q})}{\sim} B$?

Clearly, it is enough to assume that $A, B \in S_n(\mathbf{Z})$ by multiplying A and B by some positive integer t. Note that a solution to Problem 5.7 immediately yields necessary conditions for $A \overset{O(\mathbf{Z})}{\sim} B$. In the following case a solution to Problem 5.7 is relatively simple:

THEOREM 5.8. *Let $A, B \in S_n(\mathbf{Z})$. Assume that A and B have the same characteristic polynomial. Suppose furthermore that*

$$\det(\lambda I_n - A) = \prod_{i=1}^{k} (\lambda - \lambda_i)^{m_i}, \qquad \lambda_i \in \mathbf{Z},\ \lambda_i \neq \lambda_j,\quad i \neq j = 1,\ldots,k.$$

Let $X_i, Y_i \subset \mathbf{Z}^n$ be the invariant sublattices of A and B corresponding to the

eigenvalue λ_i. *Denote by* E_i, F_i *the matrices given by* (4.14). *Then*

$$A \overset{O(Q)}{\sim} B \quad \Leftrightarrow \quad E_i \overset{Q}{\sim} F_i, \quad i = 1, \ldots, k. \tag{5.9}$$

Proof. Clearly, the LHS of (5.9) implies its RHS. Since X_i (Y_i) is orthogonal to X_j (Y_j) for $i \neq j$ and since $A_i = \lambda_i I$, $B_i = \lambda_i I$, the RHS of (5.9) implies its LHS. ∎

Theorem 5.8 gives rise to rational invariants of strongly regular graphs whose eigenvalues are integers. It seems that Problem 5.7 should have a reasonably nice solution in the case where $\det(\lambda I_n - A)$ splits over a quadratic extension of $\mathbf{Q}$. Such a solution will give rise to rational invariants on strongly regular graphs. Consult for example [3] for the definition and the properties of strongly regular graphs.

REFERENCES

1 J. W. S. Cassels, *Rational Quadratic Forms*, Academic, 1978.
2 J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, Springer, 1988.
3 D. M. Cvetkovic, M. Doob, and H. Sachs, *Spectra of Graphs*, Academic, 1979.
4 S. Friedland, Analytic similarity of matrices, in *Lecture Notes in Appl. Math.*, 18, Amer. Math. Soc., 1980, pp. 43–85.
5 S. Friedland, Normal forms for definite integer unimodular quadratic forms, *Proc. Amer. Math. Soc.* 106:917–921 (1989).
6 S. Friedland, Coherent algebras and the graph isomorphism problem, *Discrete Appl. Math.* 25:73–98 (1989).
7 F. R. Gantmacher, *The Theory of Matrices*, Vol. I, Chelsea, 1959.
8 M. R. Garey and D. S. Johnson, *Computers and Intractability: a Guide to NP-Completeness*, Freeman, 1979.
9 D. S. Johnson, The NP-completeness column: An ongoing guide, *J. Algorithms* 3:288–300 (1982).
10 R. Kannan, Improved algorithms for integer programming and related lattice problems, *15th ACM STOC Symposium*, pp. 193–206.
11 A. Lubiw, Some NP-complete problems similar to graph isomorphism, *SIAM J. Comput.* 10:11–21 (1981).
12 E. M. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, *J. Comput. System Sci.* 25:42–65 (1982).
13 J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, 1973.
14 P. Sarnak, Some applications of modular forms, preprint.
15 J. P. Serre, *A Course in Arithmetic*, Springer, 1973.

Received 20 October 1989; final manuscript accepted 25 October 1990